基于区块链的数字货币演化

谢开斌 [1, 2]

(1. 京北方信息技术股份有限公司, 北京 100089; 2. 中国科学院计算技术研究所 中国科学院智能信息处理重点实验室, 北京 100190)

摘　要：区块链是数字货币研究的主流技术和重要前提。作为一种去中心化的分布式计算技术，区块链具有共同维护、防篡改、可追溯等中心化技术所不具备的优势。以区块链的基本原理为基础，主要分析了哈希加密、共识机制以及智能合约方面的关键技术；以区块链中的首个应用比特币为基础，，分析了以太坊、达世币、卡尔达诺、比特股等数字货币的发展演化历程。根据数字货币的研究现状及其所面临的诸多挑战，展望了区块链未来在数字货币的发行与监管、交易跟踪和海量交易数据分析方面的研究趋势。

关键词：区块链；去中心化；比特币；数字货币；演化

中图分类号：TP301　　doi: 10.3969/j.issn.1001-3695.2018.03.0258

Study on evolution of digital currency based on blockchain

Xie Kaibin[1, 2]

(1. *Northking Information Technology Co. Ltd*, *Beijing* 100089, *China*; 2. *Key Laboratory of Intelligent Information Processing of Chinese Academy of Sciences*, *Institute of Computing Technology*, *Chinese Academy of Sciences*, *Beijing* 100190, *China*)

Abstract: Blockchain is the mainstream technology and important premise of digital currency. As a decentralized, distributed computing technology, blockchain is better than concentrated distribution in joint maintenance, tamper-resistant, traceable and so on. Based on the basic principle of blockchain, the key technologies of blockchain were mainly studied in hash encryption technology, consensus mechanism and smart contracts. On the basis of the Bitcoin which is the first application of blockchain, the evolution of Ethereum, Dash, Cardano and BitShares were analyzed. According to the current researches and challenges of digital currency, issuance and regulation of digital currency, transaction tracking and the analysis of massive transaction data were proposed as the future research trends of blockchain.

Key words: blockchain; decentralized; Bitcoin; digital currency; evolution

0　引言

21 世纪以来，随着普适计算技术、网络技术和人工智能技术的不断进步，金融业得到了快速的发展，应用领域也越来越广泛。然而，基于金融业所进行的交易主要依赖第三方机构来进行处理，如银行、保险、交易所等平台，即需要一个中心化的可信机构做担保。这种以第三方作为中介的交易模式尽管在绝大多数情形下表现良好，但存在着以下的主要问题：a）中心化机构内部的操作不透明，存在着内部人员进行暗箱操作的金融风险；b）中心化机构的建设及维护成本高，需要巨额资金；c）中心化机构容易成为网络黑客的攻击目标，需要时刻防范黑客可能发起的网络攻击。

为了解决中心化机构存在的上述种种问题，一个化名中本聪的研究人员创新性的提出了颠覆中心化架构的区块链技术，并开发了首个基于区块链的应用：比特币。区块链和比特币的核心思想体现在文献《Bitcoin: a peer-to-peer electronic cash system》[1]。该论文首次对区块链进行了如下的定义：通过为包含交易事件的区块进行哈希运算，从而为区块添加时间戳特征，并广播区块的哈希值，以达成对区块内交易确认的共识，并根据与时间戳对应的哈希值将不同的区块按时间顺序链接起来，形成一个不断变长的交易记录链条[1]。

随着越来越多的科研人员加入到区块链的研究中来，区块链中的哈希加密技术、共识机制以及智能合约等核心技术都得到了深入的研究。哈希加密技术确保了区块内的交易的安全性以及相邻区块之间链接的有效性[2,3]。共识机制主要解决了如何激励分布式个体加入区块链生态系统以及增强交易可靠性的问题[4,5]。智能合约技术是虚拟空间与物理空间之间的桥梁，使得人们在物理空间达成的合约能够通过虚拟空间的智能技术

收稿日期：2018-03-05；**修回日期：**2018-05-07

作者简介：谢开斌（1981-），男，博士（后），主要研究方向为区块链和物联网（xkbzcxkb3@sina.com）.

实现[6-7]。

比特币作为首个采用区块链技术并成功运行的数字货币，其市值已达到了上千亿美金，但在九年多的运行过程中，其在交易速度、交易确认时间、能源消耗、应用可扩展性和存储安全等方面的不完善之处也逐渐显现。为了对比特币的上述不完善之处进行改进，比特币之后开发的以区块链技术为基础的数字货币，如以太坊（Ethereum）、达世币（Dash）、卡尔达诺（Cardano）以及比特股（BitShares）等都对比特币进行了一定程度的改进和演化，推动了数字货币在使用便捷性、应用的多样化性和数字货币的安全存储性等方面的进一步发展。

1　区块链的基本原理及关键技术

区块链作为一种去中心化的分布式系统的关键技术，成功的实现了在无中心化机构背书的前提下，节点与节点之间可以进行可信的交易。这是由于区块链采取了适应 P2P 交易的数据结构[8-10]，才使其成功的实现了去中心化。此外，哈希加密技术、共识机制和智能合约技术等都是区块链技术飞速的发展的关键，促进了基于区块链的数字货币的基础理论研究及应用的发展。

1.1　区块链的基本原理

区块链中区块的基本结构由四部分组成，分别是区块分隔符、区块大小、区块头部和区块体。图 1 说明了区块整体的基本结构。其中区块大小决定了区块中所能记录的交易的数量；区块头部用来链接其紧邻的区块；区块体内记录了所有需要被验证的交易。

区块分隔符（4字节）
区块大小（4字节）
区块头部（80字节）
区块体（不确定）

图 1　区块的基本结构

区块头部由以下六部分组成，分别是：区块版本号、父区块哈希值、Merkle 树根值、时间戳、目标值以及随机数。区块头部通过父区块哈希值实现了相邻区块之间的链接。区块头部的结构如图 2 所示。

区块版本号（4字节）	父区块哈希值（32字节）
Merkle树根值（32字节）	时间戳（4字节）
目标值（4字节）	随机数（4字节）

图 2　区块头部

区块体由两部分组成，分别是区块的交易记录以及每条交易记录的详情。区块的交易记录如图 3 所示。

货币版本号（4字节）	发送交易数量（>1字节）
接收交易数量（>1字节）	货币发送地址(>40字节）
货币接收地址(>40字节)	交易时间戳(4字节）

图 3　交易记录

1.2　区块链的关键技术

区块链是未来交易信息存储和查询的重要技术，基于其的关键技术正从理论研究走向具体应用。目前，区块链的三个主要关键技术分别是哈希加密技术、共识机制以及智能合约技术。下面对这三个关键技术进行剖析和说明。

1.2.1 哈希加密技术

哈希加密技术以哈希加密算法为基础，是区块链系统安全的重要保障技术之一。哈希加密技术具有下述的四个方面的特性，使得其非常适用于区块链领域。这四个方面的特性描述如下：

a）破解困难。对哈希加密后的信息进行逆向推算需要的时间是天文数量级，因此几乎不可能破解哈希加密信息。

b）加密或验证简单。给定要加密的信息与对应的哈希算法，能够在非常短的时间内对信息进行加密。或者给定加密后的信息，很容易验证其是否是某段信息的哈希加密结果。

c）信息敏感性。加密信息即使只进行了轻微的改变，则其经过哈希加密运算后得到的值也会发生根本的变化。

d）加密结果无冲突。不同的加密信息经过哈希算法运算后，不可能产生相同的哈希值。

此外，在区块链中利用 Merkle 哈希树[11, 12]可以验证交易数据是否被篡改或删除。Merkle 哈希树是一类以哈希运算为基础的树，通常为二叉树，也可以是多叉树，树上的叶子结点为交易数据的哈希值，非叶子节点是其孩子节点的哈希块连接在一起进行哈希后的值。Merkle 哈希树的树根可以用来验证交易数据的完整性以及交易数据是否被篡改过，而且验证过程所需要的数据传输量及数据计算量是很低的，通常是对数数量级。MERKLE 哈希树的结构如图 4 所示。

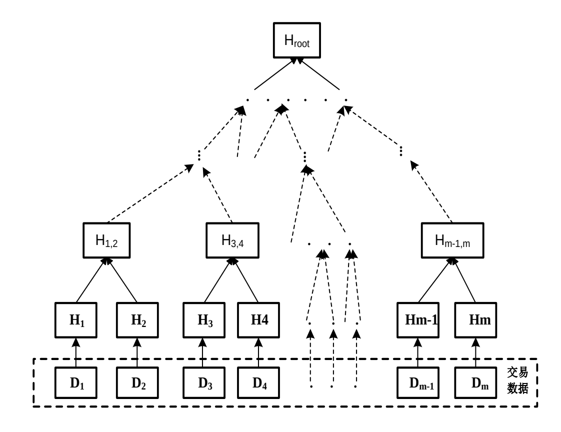


图 4　Merkle 哈希树的结构

1.2.2 共识机制

共识机制主要是为了解决在去中心化的场景下如何让区块链中的分布式节点之间互相信任的问题，而且也是保证区块链系统能够持续运行的关键。目前的共识机制主要有工作量证明机制（PoW）、股权证明机制（PoS）、股份授权共识机制（DPoS）、拜占庭容错机制（PBFT）等。

PoW 的核心思想是让工作量越大的节点收益越高，即收益与工作量大小近似成正比[13]。该机制正是依靠强大的工作

量确保区块链的安全性。但是该机制也有明显的缺陷即大量的资源耗费；以及工作量计算所造成的交易等待时间较长。比特币就采用了 PoW；让所有节点求解复杂但易于验证的数学难题。通常只有算力最高的节点才能解开难题，获得若干比特币的奖励[14]。

PoS 是用“拥有的币龄”的多少来证明节点是否有资格进行记账。其目的是尽可能的减少资源的消耗，而又能达成共识。该算法让具有最多币龄的“记账人”节点负责创建区块，且享有投票权[15]。相比 PoW，PoS 最大的优点是缩短了共识达成的时间和减少了能源的消耗；但也造成了拥有资源或币龄少的节点几乎永远不可能获得记账权和投票权[16]。卡尔达诺（Cardano）采用了 PoS 机制,以太坊（Ethereum）计划未来也采用该机制。

DPoS 是一种股份授权证明机制，类似于公司董事会投票；其机制是让每一个节点选出候选人，让候选人作为代表进行记账和投票[17]。由此可以看出，DPoS 从一定程度上减少了参与记账和验证的结点个数，且让每一个节点都可以参与到记账和投票中来。因此，DPoS 在某种程度上是一种结合了 PoW 和 PoS 的优势的机制。目前比特股（BitShares）等都采用了该机制[18]。

PBFT 实现了一种拜占庭容错的分布式文件系统，该机制能够保证系统的活性和安全性且提供了很高的容错性[19]。一般在该机制中的失效节点数只要小于系统节点总数的 1/3 就能保证系统的安全性和活性。这里的活性指的是系统中的节点发送消息后都会收到响应；安全性指的是复制副本满足线性一致性。该机制通常用使用在私有链上。

除了上述四种主要的共识机制外，目前国内也提出了两种主要的共识机制：授权拜占庭容错算法（dBFT）[20]和 POOL 验证池算法[21]。dBFT 对 PBFT 机制进行了改进，其核心思想是：根据节点权益来选择区块的记账人，然后记账人之间的记账权通过拜占庭容错算法来达成共识。POOL 验证池算法是在一致性算法 Pasox 等的基础上，结合数据验证机制实现的快速共识算法。

1.2.3 智能合约技术

智能合约技术是跨领域学者尼克•萨博（Nick Szabo）首先提出来的，并给了智能合约如下的定义：一套以数字形式定义的承诺（promises），包括合约参与方可以在上面执行这些承诺的协议[22]。在区块链领域，智能合约用来封装区块链系统中的各类脚本代码。这些脚本代码规定了合约中的交易的执行方式及交易的具体内容。智能合约使得区块链可以成为一种可编程的货币，而且比传统的货币交易更加灵活和高效。通常在合约中可以设置合约的执行时间、合约的触发规则等。数字货币中的以太坊等都实现了智能合约的功能。

基于区块链的智能合约的构建及执行通常包括如下的三个步骤：

a）产生合约，根据合约参与方的需要，设计脚本代码来实现合约的内容；

b）合约的存储，实现合约的脚本代码需要存储到区块链的块中；

c）合约的执行，合约的脚本代码要能自动的执行，而无需人为的干预或操作。

2　基于区块链的数字货币的演化

区块链技术发展至今，已经出现了上千种的以区块链为设计基础的数字货币。这些数字货币都以区块链中的首个应用，即比特币(Bitcoin)为原型，对 Bitcoin 在功能或性能等不完善的方面进行了一定程度的演化，以此来满足各种应用场景的需求。

Bitcoin 的设计原理如下：一个建立在 P2P 协议和椭圆曲线签名算法（ECDSA）[23]基础上的加密数字货币，该数字货币需要由“矿工”通过挖矿，即获取满足区块头部难度系数的哈希值；每个区块附带的数字货币数量初始为 50 个，且每四年减半，从而保证 Bitcoin 有确定的上限。

Bitcoin 作为一种以密码学为理论基础的数字货币，取得了巨大的成功，但在约九年的运行过程中，其不完善之处也逐渐显现，主要体现在下述几个方面：

a）基于 Bitcoin 的交易速度慢。比特币由于十分钟左右才出一个块，块大小仅有 1M 且得经过连续六个区块的确认才能生效，因此交易时间通常长达数个小时，远达不到目前商业交易的要求。

b）生成 Bitcoin 需要耗费大量的能源。Bitcoin 的生成采用基于 PoW 的共识算法，需要进行大量的运算，耗费的电能是巨量的。

c）应用单一化。Bitcoin 由于其功能相对单一，其除了与法定货币或其他数字货币进行交易或交换外，要进行其他方面的应用开发难度通常很大。

d）存储安全性有待加强。Bitcoin 交易所以及个人保存的 Bitcoin 近年来多次遭到黑客的攻击，造成 Bitcoin 被窃和用户的恐慌，影响了 Bitcoin 的推广。

e）监管缺失，成为洗钱工具。由于 Bitcoin 的私钥只有拥有者自己知道，且拥有者的身份等都是匿名的，因此很容易被不法分子作为洗钱的工具。

f）去中心化程度的削弱。随着 Bitcoin 中“挖矿”的矿场的规模越来越大，大的矿场的算力远远高于小矿场和个人的算力，且几个大矿场的联合算力已超出总算力的 50%，这使得经济实力薄弱的个体和小团体不得不退出挖矿，背离了 Bitcoin 的去中心化的初衷。

由于 Bitcoin 存在上述六个方面的不完善之处，后来陆续开发的数字货币系统，如 Ethereum、Cardano、Dash、BitShares 等以 Bitcoin 为基础，对 Bitcoin 在功能上进行了演化，分别在一定程度上解决 Bitcoin 存在的上述若干问题。下面分别对这几类数字货币系统的设计原理进行介绍，并说明它们与 Bitcoin 相比在那些方面进行了完善和演化。

2.1 以太坊（Ethereum）

Ethereum 是以 Bitcoin 为基础的一个区块链应用开发平台，能够适应不同的操作系统和开发语言，具有多样化的客户端。Ethereum 使用 Python、C、Java 等语言来开发区块链应用；这些应用所使用的高级语言通过各自的编译器转化为图灵完备的脚本语言（Ethereum virtual machine，简称为 EVM 语言）去执行[24]。

Ethereum 与 Bitcoin 最大的一个区别是其提供了功能强大的智能合约编程环境。如果说 Bitcoin 的功能只是局限在数字货币本身的使用价值上，即通常认为的区块链 1.0；那么 Ethereum 根据各类应用在商业与非商业环境下的复杂逻辑，可以开发出满足各种需求的智能合约应用程序，极大的丰富了数字货币的应用领域，直接将区块链技术的发展带入到区块链 2.0 时代。

Ethereum 与 Bitcoin 相比，其进行演化的地方主要体现在以下几点：

a)多样化的应用开发：智能合约使得 Ethereum 上的应用众多，极大的开拓了数字货币的应用领域和使用范围。

b)交易速度的加快：Ethereum 的出块只需要十几秒，比 Bitcoin 的出块速度要快一个数量级，因此其交易速度比 Bitcoin 快。

c)增强了去中心化的程度：Ethereum 采取 SHA-3 哈希算法，可以阻止使用 ASIC 挖矿，使得超级矿机出现的难度增大，从而能使得更多的“矿工”加入以太币挖矿,增强了 Ethereum 的去中心化程度。

2.2 卡尔达诺（Cardano）

Cardano 是数字货币行业内首个先做数字货币的学术研究，再根据发表后的研究成果去实现加密数字货币，即 Cardano 数字货币系统。由此可以看出，Cardano 的性质及其功能都是经过严格的数学证明和学术界同行的评审，保证了其在理论上是安全和正确的。

Cardano 采用的共识机制是 PoS，该机制的具体实现协议名为乌洛波罗斯（Ouroboros）[25]且该协议使用经过严格的数学证明,确保其安全性是有理论保证的。

Cardano 采用分层架构进行实现，主要的功能层如下[26]：a)清算层,Cardano 的代币在该层流通,是 Cardano 整个生态系统的基础，是为了实现对 Cardano 币的交易量、交易时间等信息的记录；b）计算层,在该层提供智能合约、消息认证、消息通信等功能，以方便应用开发者在这一层开发满足各种需求的应用。

Cardono 的一项重大创新就是计划采用形式化方法来完成受控计算，从而实现用户隐私和监管需之间的平衡；进而试图减少使用 Cardano 所存在的金融风险。此外，Cardano 计划使用不同于 TCP/IP 的递归网络架构（Recursive InterNetwork Architecture，RINA)[27]，使得节点之间的信息交互类似于进程间交互，以加快节点之间的信息传递效率。

Cardano 与 Bitcoin 相比，其进行演化的功能主要体现在以下几点：

a)交易速度的提升。Cardano 功能的分层实现以及采取 RINA 架构，使得 Cardano 的交易速度得到了极大的提升。

b)Cardano 采用 PoS 共识机制，极大地降低了能源的消耗。

c)使得对数字货币的监管成为可能。Cardono 在形式化的推理设计中，考虑了对数字货币的金融监管。

d)多样化的应用开发。智能合约功能丰富了基于 Cardano 的应用开发。

e)增强了数字货币的存储安全性。Cardano 的形式化实现方法有利于设计与其匹配的存储方案。

2.3 达世币（Dash）

Dash 是 Bitcoin 的超集，具有 Bitcoin 的主要特性，例如其也要进行挖矿来产生达世币，只是达世币中出块的速度为约每 2.5 分钟产生一个块，奖励给挖出该块的矿工 5 个达世币。

Dash 对 Bitcoin 的最大扩展之处在于增加了主节点网络[28]。Dash 中的节点如果拥有了 1000 个用来进行资质认证的达世币，其就可以作为主节点。主节点网络以 Bitcoin 的底层区块链网络为基础，由专用服务器组成。目前主节点网络中的主节点总数超过了四千。

Dash 将“挖矿”产生的达世币按照 45%、45%、10%的比例分配给“矿工”、对交易进行确认的主节点以及达世币社区。由于主节点网络的存在，Dash 内的交易交易可以在几秒内完成，即实现即时支付；而且由于有主节点网络的信用背书，能大大增强交易的安全性。DASH 中的社区为区块扩容、生态链发展等方面问题提供了一个解决的通道。

在“挖矿”算法方面，Dash 使用 X11 算法，即使用 11 轮 SHA3 算法进行哈希运算，且每轮的计算结果都作为下一轮的输入，直到完成 11 轮的运算；这样做的目的是为了延迟针对特定算法的矿机的产生时间，使得更多的人使用普通的计算机参与到 Dash 的挖矿中来。

Dash 与 Bitcoin 相比，其进行演化的功能主要体现在以下几点：

a)商业级的交易速度。主节点网络使得交易能达到绝大多数的商业需求。

b)很高的去中心化程度。X11 算法保障更多的“矿工”可以参与到 Dash 的“挖矿中”；且 Dash 中的社区也增强了 Dash 的去中心化程度。

c)Dash 中的社区机制从一定程度上对 Dash 币的交易起到了监管作用。

2.4 比特股（BitShares）

BitShares 是一个基于区块链技术的金融交易综合服务平台，其目标是构建一个去中心化的自由市场金融生态系统。任何个人或机构都可以在 BitShares 平台上进行转账交易，发起众筹等；还可以基于 BitShares 构建虚拟货币交易所；甚至还能在 BitShares 平台上实现符合监管的黑白名单等功能。

BitShares 设计了一种可自由交易的新型数字资产：比特股市场锚定资产[29]，该类资产可以和美元，欧元或黄金等进行兑换。例如比特股数字锚定资产 BITUSD 可以兑换同等数额的美元。比特股市场锚定资产通常以两倍价值的比特股数字锚定资产作为抵押物，并以智能合约自动执行清算来保证兑换的执行，从而可以避免兑换交易的违约风险，保证了比特股市场锚定资产价值的稳定性，让比特股生态系统形成良性循环。

此外，BitShares 使用了 DPoS 的机制，让拥有比特股的节点都有权进行投票，票数最高的 101 个节点有权对交易进行记录。

Bitshares 与 Bitcoin 相比，其进行演化的功能主要体现在以下几点：

a)商业级的交易和转账速度：Bitshares 由于采用了 DPOS 机制，使得交易确认时间在 3 秒内可完成，交易速度可达每秒 10 万笔，完全达到了通常条件下的商业交易的要求。

b)几乎无需能源的消耗 DPoS 机制确保 BitShares

c)适用于多个应用领域：比特股市场锚定资产可以保证比特股的价格在一定时期内保持价格稳定，从而使其能够在多个领域内应用。

综上，Ethereum、Cardono、Dash、BitShares 在交易速度，能耗，应用多样化，存储安全性，监管以及去中心化程度方面的演化对比如表 1 所示。

表 1　数字货币演化程度对比

数字货币	交易速度	能耗	多样化程度	存储安全性	监管	去中心化程度
Ethereum	较慢	较高	高	较低	未考虑	较低
Cardano	较快	低	较高	高	可实现	高
Dash	快	高	较高	较低	可部分实现	较高
BitShares	快	高	较高	较低	未考虑	高

3　数字货币的未来研究趋势

区块链对传统中心化技术进行的颠覆性创新，为金融、食品安全、物种保护、物联网等众多行业提供了可供选择的去中心化的应用模式。根据区块链本身的特性以及区块链目前的应用现状，以下所列的研究内容预测是未来区块链研究的主要方向：

a）基于区块链的数字货币发行方面的研究：数字货币目前在发行、流通、监管、调控等方面技术尚不成熟[30,31]，缺少有效的发行方案。未来在数字货币方面的研究将会涉及如下方面：降低传统纸币发行、流通的高昂成本方面的研究，提升经济交易活动的便利性和透明度方面的研究，减少洗钱、逃漏税等违法犯罪行为方面的研究以及提升央行对货币供应和货币流通的控制力等方面的研究。

b）基于区块链的交易追踪方面的研究：目前的研究主要考虑了基于区块链的数字资产交易如何进行[32,33]，在基于区块链的交易的可追溯方面的研究还较少。未来的研究方向应该是设计交易规则和监管框架等来保证交易的高效性和追踪的及时性。

c）区块链中海量数据的分析研究：目前的研究很少有涉及到对区块链中的海量数据分析[34,35]。但是区块链中记录的数据都是物理世界中产生的真实的数据，这些数据对于用户画像和用户行为等方面的分析具有巨大的商业价值，因此，未来的研究将会是使用机器学习[36]或深度学习[37]等各类智能算法分析区块链中的用户数据，提炼出其中有价值的商业信息。

4　结束语

本文介绍了区块链技术的基本原理，分析了基于区块链的比特币的性质以及在比特币基础上开发的 Ethereum、，Cardano，Dash、BitShares 等对比特币的功能演化。以区块链技术目前的主要应用现状为基础，分析了数字货币研究面临的挑战和未来可能的研究趋势。

区块链技术从提出到现在尚不足十年，还处于非常初期的发展阶段，与其相关的标准还未成熟。尽管如此，许多国家都将区块链作为重大的战略研究技术，这是因为区块链对一个国家在金融主权、社会征信、跨境交易等领域都将产生重要且深远的影响。因此，积极参与区块链相关技术在各领域标准的制定，深入研究区块链对各领域的技术创新的价值将会增强国家未来在科技、经济等诸多领域的话语权和领导权。

参考文献：

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. (2008-11-01) [2018-05-06]. http://www. bitcoin. org/bitcoin. pdf.

[2] Devine R. Design and implementation of DDH: a distributed dynamic hashing algorithm [C]// Proc of International Conference on Foundations of Data Organization and Algorithms. Berlin: Springer, 1993: 101-114.

[3] Courtois N T, Grajek M, Naik R. Optimizing Sha256 in bitcoin mining [C]// Proc of International Conference on Cryptography and Security Systems. Berlin: Springer, 2014: 131-144.

[4] Ephrati E, Rosenschein J S. The clarke tax as a consensus mechanism among automated agents [C]// Proc of National Conference on Artificial Intelligence. Anaheim: AAAI Press//MIT Press, 1991: 173-178.

[5] Liu Yujia, Liang Changyong, Chiclana F, *et al.* A trust induced recommendation mechanism for reaching consensus in group decision making [J]. Knowledge-Based Systems, 2017, 119 (C): 221-231.

[6] Kosba A, Miller A, Shi E, *et al.* Hawk: The blockchain model of

cryptography and privacy-preserving smart contracts [C]// Security and Privacy. California: IEEE Press, 2016: 839-858.

[7] Luu L, Chu D H, Olickel H, *et al.* Making smart contracts smarter [C]// Proc of ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 254-269.

[8] Ron D, Shamir A. Quantitative analysis of the full bitcoin transaction graph [C]// Proc of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2013: 6-24.

[9] Donet J A D, Pérez-Sola C, Herrera-Joancomartí J. The bitcoin P2P network [C]// Proc of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2014: 87-102.

[10] Bhattacharya R, White M, Beloff N. A blockchain based peer-to-peer framework for exchanging leftover foreign currency [C]// Proc of Computing Conference. Hangzhou: IEEE Press, 2017: 1431-1435.

[11] Li Hongwei, Lu Rongxing, Zhou Liang, *et al.* An efficient merkle-tree-based authentication scheme for smart grid [J]. IEEE Systems Journal, 2014, 8 (2): 655-663.

[12] Ahmad A, Alajeely M, Doss R. Establishing trust relationships in OppNets using Merkle trees [C]// Proc of International Conference on Communication Systems and Networks. Beijing: IEEE Press, 2016: 1-6.

[13] Gervais A, Karame G O, Glykantzis V, *et al.* On the Security and Performance of Proof of Work Blockchains [C]// Proc of ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 3-16.

[14] Sleiman M D, Lauf A P, Yampolskiy R. Bitcoin message: data insertion on a proof-of-work cryptocurrency system [C]// Proc of International Conference on Cyberworlds. Chongqing: IEEE Press, 2016: 332-336.

[15] Li Wenting, Andreina S, Bohli J M, *et al.* Securing Proof-of-Stake Blockchain Protocols [M]// Data Privacy Management, Cryptocurrencies and Blockchain Technology. Cham: Springer, 2017: 297-315.

[16] Bartoletti M, Lande S, Podda A S. A Proof-of-stake protocol for consensus on bitcoin subchains [C]// Proc of International Conference on Financial Cryptography and Data Security. Cham: Springer, 2017: 568-584.

[17] Larimer D. Delegated proof-of-stake (dpos) [EB/OL]. (2013-09-11) [2018-05-06]. https://bitshares. org/technology/delegated-proof-of-stake-consensus.

[18] Zheng Zibin, Xie Shaoan, Dai Hongning, *et al.* An overview of blockchain technology: Architecture, consensus, and future trends [C]// Proc of IEEE International Congress on Big Data. Honolulu: IEEE Press, 2017: 557-564.

[19] Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery [J]. ACM Trans on Computer Systems, 2002, 20 (4): 398-461.

[20] 分布科技公司. 小蚁共识算法 [EB/OL]. (2016-01-11) [2018-05-06]. http://www. onchain. com/paper/66c6773b. pdf.

[21] 布比 (北京) 网络技术有限公司. 布比区块链产品白皮书 [EB/OL]. (2016-08-21) [2018-05-06]. http://www. bubi. cn/whitePaper/index. jhtml.

[22] Szabo N. Formalizing and securing relationships on public networks [J]. First Monday, 1997, 2 (9): 1-21.

[23] Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA) [J]. International Journal of Information Security, 2001, 1 (1): 36-63.

[24] Hirai Y. Defining the Ethereum Virtual machine for interactive theorem provers [C]// Proc of International Conference on Financial Cryptography and Data Security. Cham: Springer, 2017: 520-535.

[25] Kiayias A, Russell A, David B, *et al.* Ouroboros: a provably secure proof-of-stake blockchain protocol [C]// Proc of International Cryptology Conference. Cham: Springer, 2017: 357-388.

[26] Guides T S. Why Cardano ADA Deserves Attention–Cardano Cryptocurrency Strategy [EB/OL]. (2018-01-09) [2018-05-07]. https://cardanodocs. com/introduction.

[27] Vrijders S, Staessens D, Colle D, *et al.* Experimental evaluation of a Recursive InterNetwork Architecture prototype [C]// Proc of Global Communications Conference. Washington DC: IEEE Press, 2015: 2017-2022.

[28] Robert W. Understanding the Governance and Budget System [EB/OL]. (2008-05-04) [2018-05-07]. https://dashpay.atlassian.net/wiki/spaces/DOC/pages.

[29] Schuh F, Larimer D. BitShares 2. 0: Financial Smart Contract Platform [EB/OL]. (2015-12-20) [2018-05-06]. http://docs. pybitshares. com/en/latest.

[30] Aste T, Tasca P, Matteo T D. Blockchain Technologies: The Foreseeable Impact on Society and Industry [J]. Computer, 2017, 50 (9): 18-28.

[31] Spearpoint M. A Proposed Currency System for Academic Peer Review Payments Using the BlockChain Technology [J]. Publications, 2017, 5 (3): 19.

[32] Godfrey-Welch D, Lagrois R, Law J, *et al.* Blockchain in Payment Card Systems [J]. SMU Data Science Review, 2018, 1 (1): 3.

[33] Kisore N R, Sagi S. A secure SMS protocol for implementing digital cash system [C]// Proc of International Conference on Advances in Computing, Communications and Informatics. Kerala: IEEE Press, 2015: 1883-1892.

[34] Kuzuno H, Karam C. Blockchain explorer: An analytical process and investigation environment for bitcoin [C]// Electronic Crime Research. Arizona: IEEE Press, 2017: 9-16.

[35] Vo H T, Mehedy L, Mohania M, *et al.* Blockchain-based Data Management and Analytics for Micro-insurance Applications [C]// Proc of ACM Conference on Information and Knowledge Management. New York: ACM Press, 2017: 2539-2542.

[36] Adoma F. Big data, machine learning and the blockchain technology: an overview [J]. International Journal of Computer Applications, 2018, 180 (28): 1-4.

[37] Gimpel H, Röglinger M. Disruptive technologien: blockchain, deep learning & Co [J]. Wirtschaftsinformatik & Management, 2017, 9 (5): 8-15.